

1        **DIGITAL SIGNATURE SYSTEM, DIGITAL SIGNATURE METHOD,**  
2        **DIGITAL SIGNATURE MEDIATION METHOD, DIGITAL SIGNATURE**  
3        **MEDIATION SYSTEM, INFORMATION TERMINAL AND STORAGE MEDIUM**

4        FIELD OF THE INVENTION

5        The present invention relates to a digital signature  
6        method and a system therefor. In particular, the present  
7        invention relates to an effective technique applied when a  
8        document to be signed is an XML document, and when digital  
9        signature is performed using a portable device such as a  
10       PDA (Personal Digital Assistants) or a portable telephone  
11       compatible with i-mode communication.

12       BACKGROUND ART

13       As network electronic data techniques have developed,  
14       there has been an accompanying shift away from paper as  
15       information transmission media to the electronic data  
16       themselves. Generally, when paper is the medium used, the  
17       signing or the affixing of a seal is performed as a  
18       personal confirmation of the contents (information)  
19       recorded on the paper. However, since electronic data are  
20       easily copied and during the communication process there  
21       are many opportunities for the alteration of data, an  
22       indispensable need exists for a digital signature  
23       technique that affords high security.

1 Public key cryptography (also called asymmetric  
2 cryptography) and secret key cryptography (also called  
3 symmetric cryptography) are well known data cryptography  
4 methods. According to secret key cryptography, a sender  
5 and a recipient who engage in secure communication each  
6 hold a shared key. When communicating with the recipient,  
7 the sender uses the shared key to encrypt information, and  
8 upon receiving the encrypted information, the recipient  
9 uses the shared key to decrypt it. As an assumption when  
10 this method is employed, the shared key is a secret that  
11 is jointly shared by the sender and the recipient, and if  
12 the secret, the shared key, is compromised, encrypted  
13 communications for which the shared key is used will not  
14 be secure.

15 On the other hand, according to the public key  
16 cryptography, a pair of keys, a public key and a private  
17 key, are employed, and information encrypted using one key  
18 can not substantially be decrypted unless the other key is  
19 used. A user encrypts information using the public key of  
20 another user that has been obtained in advance, and  
21 transmits the encrypted information to the subject user.  
22 Thereafter, the recipient decrypts the received  
23 information using his or her private key. The advantage  
24 of this method is that communication security can be  
25 maintained even when the public key has been disclosed to  
26 third parties, and no secret key information need be  
27 shared as a communication prerequisite. A digital  
28 signature can also be affixed using this public key  
29 cryptography. That is, a sender, using a private key that

1 only he or she has knowledge of, can encrypt a document,  
2 and a recipient can obtain a public key corresponding to  
3 the private key and use it to decrypt the document. As a  
4 result, the contents of the signed document can be  
5 confirmed. In this case, satisfactory grounds must be  
6 established to confirm that the disclosed public key  
7 belongs to the signing person. For this confirmation, a  
8 certification service provided by a certification  
9 authority (CA) can be employed. For the user, it is  
10 important that he or she be able to protect his or her  
11 private key. If the private key should be exposed, a  
12 third party could employ the private key to impersonate  
13 the actual owner of the key. Therefore, for the security  
14 of a digital signature (both for communication  
15 cryptography and key distribution) it is imperative that  
16 absolute protection be afforded a private key.

17 For recent electronic commerce (e-business), XML documents  
18 have been employed as the form used for the exchange of  
19 data. Since an XML document is a self-descriptive  
20 structure, more complicated data can be handled  
21 effectively. Therefore, it is highly possible that XML  
22 will be employed as a standard not only for B2B (business  
23 to business) documents, but also B2C (business to  
24 consumer) documents.

25 Because of this background, digital signature  
26 specifications for XML, XMLDSIG, are being established for  
27 the WWW Consortium, W3C. The XML digital signature  
28 technique is expected to be used as a trump card for the

1 prevention of data alteration and the acquisition of  
2 evidence to support a transaction.

### 3 Problems to be Solved by the Invention

4 As is described above, the protection of a private key is  
5 important in order to prove the identity of an  
6 authenticated user, or to prevent a third party from  
7 impersonating the authenticated user. Thus, it is not  
8 secure for a private key to be stored and managed on the  
9 hard disk of a personal computer; it is advantageous that  
10 the private key be stored on a security token, such as a  
11 smart card, that a user can remove and carry.

12 However, since a smart card does not have a display  
13 function, the user must employ a personal computer having  
14 a card reader to confirm, on its screen, the contents of a  
15 document to be signed. When, for example, a user  
16 purchases a product at a shop and signs a transaction  
17 document for electronic payment, the user confirms the  
18 contents of the document on the screen of a local personal  
19 computer or the POS terminal at the shop. At this time, a  
20 question exists relative to the validity of the contents  
21 of the displayed document. In this case, if the contents  
22 of the document transmitted by a transaction organization  
23 to the terminal were altered before transmission, this  
24 alteration would not be apparent to the user, who would  
25 sign a document including terms differing from those  
26 previously agreed upon. To remove this uncertainty, it is  
27 advantageous that the user employ a fully secure terminal,

1 e.g., his or her own PDA or i-mode portable telephone, to  
2 confirm a document to be signed.

3 However, the following problem has arisen relative to the  
4 mounting of a digital signature function on a terminal.  
5 This is an outstanding problem, especially when a portable  
6 terminal is used to perform the XML digital signature  
7 function, which in the future will be further developed.  
8 Since a portable terminal has only a small display screen,  
9 it is difficult to display complete sentences contained in  
10 a document that is to be signed. Especially for an XML  
11 document, the display screen of a portable terminal is  
12 insufficiently large to display additional tag information  
13 and other information based on DSIG specifications.

14 Further, the calculation resources available to a portable  
15 terminal are generally limited, and this, imposes an  
16 exceedingly large load on the portable terminal when  
17 calculations required for an electric signature are to be  
18 performed. Since especially for an XML digital signature  
19 an XML or an XPath processor is required, if such a  
20 processor is mounted on a portable terminal having only  
21 limited calculation resources, costs will be increased.

## 22 SUMMARY OF THE INVENTION

23 It is, therefore, one aspect of the present invention to  
24 provide XML digital signature technique and systems for  
25 using an information terminal, such as a portable

1 telephone, having limited calculation resources.

2 It is another aspect of the present invention to provide a  
3 more secure digital signature method and system, or a  
4 terminal for digital signatures.

5 BRIEF DESCRIPTION OF THE DRAWINGS:

6 These and other aspects, features, and advantages of the  
7 present invention will become apparent upon further  
8 consideration of the following detailed description of the  
9 invention when read in conjunction with the drawing figures,  
10 in which:

11 Fig. 1 is a block diagram showing an example digital  
12 signature system according to the present invention;

13 Fig. 2 is an example flowchart for a signature method  
14 according to one embodiment of the invention;

15 Fig. 3 is a flowchart for an example signature operation;

16 Fig. 4 is a list showing an example document to be signed;

17 Fig. 5 is a list showing example summary text;

18 Fig. 6 is a list showing a signature template; and

19 Fig. 7 is a list showing an example signed document that  
20 is generated.

1 DESCRIPTION OF THE SYMBOLS

- 2 1: Internet
- 3 2: Signature demandant system
- 4 3: Agent system (agent)
- 5 4: User terminal
- 6 5: Internet service provider (ISP)

7 DETAILED DESCRIPTION OF THE INVENTION

8 According to an example of a digital signature method of  
9 this invention, an agent acts for a signatory by receiving  
10 a document, such as an XML document, to be signed, and  
11 generates summary text of the document. The agent then  
12 transmits the summary text to the signatory, who displays  
13 it on his or her information terminal and confirms its  
14 contents. After confirming the contents, the signatory  
15 signs (encrypts) the summary text, using the private key  
16 stored in his or her terminal. Thereafter, the signatory  
17 transmits the signature value (encrypted data) to the  
18 agent, who generates a signed document, including the  
19 signature value, and transmits this to a signature  
20 demandant. Finally, the signature demandant verifies  
21 (decrypts) the received signed document using the public  
22 key of the signatory and confirms the contents.

23 According to this signature method, the user (signatory)

1 can display summary text that has been converted into a  
2 form (e.g., text form) that is appropriate for a display  
3 terminal, and can confirm the contents of a document.  
4 Furthermore, the calculation load, such as the use of the  
5 XML processor, is not imposed on the user for the  
6 cryptography of summary text, and even a device, such as a  
7 portable terminal, having limited calculation resources  
8 can satisfactorily encrypt summary text. Since the user  
9 employs his or her own terminal, the validity of the  
10 displayed data is unquestionable, and since the private  
11 key is stored in the user's own terminal, the security of  
12 the private key can be fully maintained. As a result, a  
13 secure digital signature method can be provided, according  
14 to which a signatory is responsible for the contents of  
15 the summary text, while for the contents of a document to  
16 be signed that are not included in summary text, the agent  
17 and the user (signatory) share responsibility within a  
18 range agreed upon by the agent and the user.. The summary  
19 text is generated by employing, for example, the XPath of  
20 an XML document, and for extracting the contents  
21 (character string) of the XML element. XML digital  
22 signature permits the usage of the XPath, and the thus  
23 prepared document, bearing an XML digital signature, will  
24 conform to the standards established for XML digital  
25 signature.

26 For signing summary text, a hash value (digest value) is  
27 often generated using a function, such as a unidirectional  
28 hash function, that is employed to generate for input data  
29 a uniquely representative value that is difficult to use

1 for the regeneration of the data. Then, the document,  
2 including the digest value, can be encrypted using the  
3 private key in the terminal. Additionally, a signature  
4 template, which includes a variable field to which the  
5 hash value (digest value) of the summary text is added,  
6 can be stored in the terminal. To obtain a signature  
7 value, a hash conversion can be performed for the  
8 signature template and the obtained hash value then  
9 encrypted. The URI of the document to be signed (digital  
10 document) can also be added to the signature template.

11 By using the above signature template, a signature process  
12 that conforms to the XML digital signature standards can  
13 be performed, without mounting the XML processor or the  
14 XPath processor on a terminal. That is, a signature  
15 template can be prepared in advance using a form that  
16 conforms to the XML digital signature standards, and can  
17 be recorded in the terminal. Then, for an XML signed  
18 document, a required signature value can be generated that  
19 is later added to an XML signed document that is generated  
20 by an agent. In other words, the terminal need only  
21 perform the generation of a hash value for summary text,  
22 the adding of the hash value to the template (and the  
23 adding of the URI), the generation of a hash value for the  
24 template and the cryptography of the hash value. A  
25 function, such as is supplied by the XML processor, is not  
26 required.

27 In some embodiments, the signature template is  
28 canonicalized (normalized) using a predetermined

1 algorithm. Thus, fluctuations in a document, such as  
2 blanks or symbols, can be standardized.

3 An advantageous embodiment of the present invention will  
4 now be described in detail while referring to the  
5 accompanying drawings. It should be noted, however, that  
6 the present invention is not limited to this embodiment,  
7 and that it can be implemented with various different  
8 embodiments. The same reference numerals are used  
9 throughout to denote corresponding or identical  
10 components.

11 For this embodiment, the explanation given will be mainly  
12 for the method or the system of the invention; however, as  
13 will be apparent to one having ordinary skill in the art,  
14 the present invention can be provided not only as a method  
15 and a system but also as a storage medium on which a  
16 computer-readable program can be stored. Therefore, the  
17 present invention can be implemented as hardware or  
18 software, or as a combination of the two. An example  
19 storage medium on which the program can be recorded is an  
20 arbitrary computer-readable storage medium, such as a hard  
21 disk, a CD-ROM, an optical storage device or a magnetic  
22 storage device.

23 Further, in this embodiment, a common computer system can  
24 be employed. The computer system used for this embodiment  
25 comprises a central processing unit (CPU), a main memory  
26 (RAM) and a nonvolatile memory (ROM), all of which are

1 interconnected by a bus. In addition, a co-processor, an  
2 image accelerator, a cache memory and an input/output  
3 controller (I/O) may be connected to the bus. Further, an  
4 external storage device, a data input device, a display  
5 device and a communication controller are connected to the  
6 bus via an appropriate interface. Furthermore, this  
7 computer system can also include a hardware resource with  
8 which a computer system is generally equipped. An example  
9 external storage device can be a hard disk drive; however,  
10 the external storage device is not thereby limited, and  
11 may include a magneto-optical storage device, an optical  
12 storage device, or a semiconductor storage device, such as  
13 a flash memory. The data input device can be an input  
14 device, including a keyboard, or a pointing device, such  
15 as a mouse. The data input device can also include an  
16 image reader, such as a scanner, or a voice input device.  
17 An example display device can be a CRT, a liquid crystal  
18 display device or a plasma display device. Further, the  
19 computer system can be an arbitrary type of computer, such  
20 as a personal computer, a workstation or a main frame  
21 computer.

22 Fig. 1 is a block diagram showing an example digital  
23 signature system according to the invention. The digital  
24 signature system of this embodiment comprises a signature  
25 demandant system 2, an agent system 3 and a user  
26 (signatory) terminal 4, all of which are connected to the  
27 Internet 1. In this embodiment, the Internet 1 is  
28 employed; however, the signature demandant system 2, the  
29 agent system 3 and the user terminal 4 may be connected by

1 a wired or wireless private network. Further, instead of  
2 the Internet 1, a private intranet that only a specific  
3 users can access may be employed. So long as the systems  
4 and the terminal can be interconnected by some  
5 communication means, such a configuration is included in  
6 the present invention. The signature demandant system 2,  
7 which is a system for a person who requests a signature,  
8 issues a document to be signed. The document to be signed  
9 is an XML document, as will be described in detail later.  
10 As is described above, general computer system can be used  
11 for the signature demandant system 2. The signature  
12 demandant system 2 is, for example, an electronic commerce  
13 site (EC site). As will be described later, this  
14 invention can be employed for a case wherein a signature  
15 is requested for an order slip upon the sale of a product  
16 (a book in this embodiment) through electronic commerce.  
17 For the security of electronic commerce, it is  
18 advantageous that the EC site obtain an order invoice that  
19 an orderer (user) can not deny later i.e., an order  
20 invoice bearing the signature of the orderer, and then  
21 dispatch the product. This order invoice is an electronic  
22 document, such as an XML document, and the signature is a  
23 digital signature, such as an XML digital signature. This  
24 invention can improve the security and safety of  
25 electronic commerce transactions and can contribute to the  
26 formation of a suitable transaction order. The use of the  
27 digital signature system of this embodiment is not limited  
28 to an EC site. So long as the system of this invention  
29 can provide evidence to prevent a signatory from denying a  
30 transaction later, this system is available. The system

1 can be used, for example, for a case wherein an in-house  
2 document exchanged via the Internet or an intranet is  
3 approved. That is, signature demandant can include not  
4 only an EC site, but also any other signature demandant,  
5 such as a person who has an in-house approval right or a  
6 contract partner. The agent system 3 is a system used by  
7 an agent. The agent is a third party who mediates an  
8 agreement between a signature demandant and a signatory,  
9 and who is reliable representative for of both of them.  
10 The agent system 3 generates summary text from a document  
11 to be signed. Then, as will be described later, to obtain  
12 a signed document, the agent system 3 adds a signature  
13 value generated by the terminal 4 to a requested document.  
14 In other words, the agent system 3 requests that a user  
15 (signatory) provide a signature only for the summary text  
16 of a document to be signed, and employs the signature  
17 value to generate a signed document requested by a  
18 signature demandant. The summary text is a document  
19 obtained by conversion, so that even the user terminal 4  
20 can display the main contents of the document to be  
21 signed. Since the document is converted into summary text  
22 by an agent, the terminal 4 need only display the summary  
23 text; it does not have to display all the XML document.  
24 Thus, it is easy for a document to be displayed, even when  
25 the terminal 4 is a device, such as a PDA or a portable  
26 telephone, having a small display screen. Furthermore,  
27 the user terminal 4 encrypts summary text, and basically  
28 does not have to handle an XML document. That is, the  
29 agent system 3 requests that a user provide a signature  
30 for summary text that constitutes the substantial portion

1 of a contract (promise), and processes the formal portion  
2 for matching the XML. Therefore, an XML processor, for  
3 example, need not be mounted on a user terminal 4, and the  
4 calculation load can be reduced costs lowered. The user  
5 terminal 4 is an information terminal for a user, and can  
6 be, for example, a PDA or an i-mode portable telephone.  
7 The user terminal 4 has a small display screen, and stores  
8 the private key of the user. Since the user records his  
9 or her private key on his or her own terminal, the private  
10 key can be fully protected. For digital signature using  
11 the terminal 4, the summary text can be displayed on the  
12 screen of that terminal, so that the user can trust the  
13 displayed data. The signature template is also recorded  
14 in the user terminal 4. The function of the signature  
15 template will be described later.

16 When the user terminal 4 is a portable telephone, the  
17 portable telephone is connected to the Internet 1 via an  
18 exchange 5 belonging to a carrier (a telephone provider).  
19 When the user terminal 4 is a PDA, the PDA is connected to  
20 the Internet 1 via an Internet service provider (ISP) 5.  
21 These portable terminals may be connected directly to the  
22 Internet 1 by obtaining an IP address.

23 In this embodiment, a portable terminal, such as a PDA or  
24 a portable telephone, is used as the user terminal 4.  
25 However, instead of this, a common computer system may be  
26 employed. It should be noted that when the present  
27 invention is applied to a portable terminal having a small  
28 display screen and limited calculation resources, the

1 effects are magnified.

2 Further, in this embodiment, the agent 3 is employed as an  
3 independent system; however, the signature demandant  
4 system 2 may provide the function of the agent 3, or the  
5 carrier (telephone provider) 5 or the ISP 5 may function  
6 as the agent 3. Further, an application service provider  
7 (ASP) may include the function of the agent 3 as a part of  
8 the service it provided.

9 Fig. 2 is a flowchart showing an example signature method  
10 according to the embodiment. Fig. 3 is a detailed  
11 flowchart showing an example signed portion in Fig. 2. In  
12 Fig. 2, the process performed by the signature demandant  
13 is shown on the left, the process performed by the agent  
14 is shown in the center, and the process performed by the  
15 signatory is shown on the right.

16 First, the signature demandant system 2 generates a  
17 document to be signed (step S10).

18 Fig. 4 is a list showing an example document to be signed.  
19 As is shown in Fig. 4, the document to be signed is  
20 written in XML. A complicated transaction can be  
21 effectively performed by the information exchange of the  
22 XML document. It should be noted that on the list in Fig.  
23 4, the numbers on the left are line numbers. The same  
24 thing applies to the lists in Figs. 5 to 7. The XML  
25 document in Fig. 4 is an example book order invoice. An  
26 <invoice> tag indicates that a document is an invoice

1 (line numbers 1 to 25), and the portion enclosed by  
2 <bookorder> tags represents the contents of a book order  
3 (line numbers 3 to 10). The title, the ISBN code, the  
4 volume and the price are written as the order contents in  
5 the portions enclosed respectively by <title> tags, <ISBN>  
6 tags, <quantity> tags and <price> tags. Further,  
7 information concerning a payment is written in the portion  
8 enclosed by <payment> tags (line numbers 11 to 24). And  
9 the payment destination, the payment source, the price,  
10 the payment due date and the payment method are written in  
11 the portions respectively enclosed by <payTo>, <billedTo>,  
12 <amount>, <dueDate> and <paymentMethod> tags. In  
13 addition, payment by card and various card data are  
14 written in (line numbers 16 to 23). It should be noted  
15 that this invoice (XML document) is merely an example.

16 An explanation will now be given for a case wherein a  
17 signature demandant (a book vendor in this embodiment)  
18 prepares the above invoice, and requests a confirmation  
19 signature be applied to the invoice. The signature  
20 demandant system 2 transmits the prepared document to the  
21 agent system 3, and the agent system 3 receives the  
22 document and records it (step S11).

23 Using the document, the agent system 3 generates summary  
24 text to be signed (step S12). Fig. 5 is a list showing  
25 example summary text that has been generated. The XPath  
26 processor is employed to generate summary text. That is,  
27 the XPath processor is mounted at the agent system 3, and  
28 the summary text is automatically generated based on the

1 document to be signed (invoice in Fig. 4). As is shown in  
2 Fig. 5, the summary text is a text document that includes  
3 only the essential portion for an order and payment. The  
4 agent system 3 then transmits the summary text to the user  
5 terminal 4, and the user terminal 4 displays it (step  
6 S13). As is described above, the summary text is plain  
7 text that includes only an important portion required for  
8 confirmation. Thus, even a user terminal 4 having a small  
9 screen can fully display the summary text. The user  
10 confirms the reliable contents of the summary text  
11 displayed on the screen (step S14), and signs the summary  
12 text if he or she agrees with the contents (step S15).

13 Fig. 3 is a flowchart for the signature process. For this  
14 process, first, the digest value of the summary text that  
15 has been confirmed is calculated (step S20). The hash  
16 function, for example, is employed for the calculation of  
17 the digest value. It should be here noted that not only  
18 the hash function, but also another function can be  
19 employed that provides a unique value to be output for the  
20 input data, and further, that it is difficult to perform  
21 an inverse conversion based on the output value. Then,  
22 the digest value and the URI for signature are introduced  
23 into the signature template (step S21). Fig. 6 is a list  
24 showing an example signature template. The signature  
25 template is generated in advance to match the document to  
26 be signed (the order invoice in Fig. 4), and conforms to  
27 the XML digital signature standards.

28 Variable fields are included in the signature template

1 (line numbers 7 and 24). In this embodiment, the target  
2 URI and the digest value for the summary text are  
3 allocated to the variable fields. The digest value (hash  
4 value) of the summary text and the URI of the document to  
5 be signed are added to the variable fields. The signature  
6 template is canonicalized using a predetermined algorithm.  
7 Thus, fluctuations, such as a character code, a blank or  
8 a symbol, can be removed. Even when these slight  
9 fluctuations do not affect the contents of a document, the  
10 hash value greatly differs and interferes with the  
11 examination of the signed contents. Through  
12 canonicalization, the occurrence of this barrier can be  
13 prevented.

14 Following this, the digest value is calculated for the  
15 overall signature template to which the digest value of  
16 the summary text and the URI of the document are added  
17 (step S22). The hash function can also be employed for  
18 the calculation of this hash value. Thereafter, the  
19 digest value obtained for the overall signature template  
20 is encrypted by using the private key (step S23). This  
21 process sequence is the signature operation, and a value  
22 generated by the cryptography is employed as a signature  
23 value. The operations performed by the user terminal 4  
24 are limited to the calculation of the hash values for the  
25 summary text and the template, and the cryptography using  
26 a private key. The template is a text document written  
27 using the character code (Unicode) that is designated by a  
28 predetermined canonicalization method, and the above  
29 operations are not those using the XML processor for the

1 XML document. That is, the operations impose only a small  
2 load, so that a device having only limited resources can  
3 satisfactorily perform them. Therefore, the effects of  
4 the present invention are magnified when an information  
5 terminal such as a PDA, which possesses limited  
6 calculation resources, is employed as the user terminal 4.

7 Further, the operation performed by the user terminal  
8 should be performed in a manner that conforms to the XML  
9 digital signature specifications. The canonicalization  
10 method, the signature method, the transformation of the  
11 summary text and the digest method are designated in the  
12 specifications. These designated specifications are  
13 written in the signed document and the signature template.  
14 For example, in the signature template in Fig. 6, the  
15 canonicalization method is written on line numbers 2 to 3,  
16 and canonicalization according to the method must be  
17 performed. The signature method is written on line  
18 numbers 4 and 5, and the DSA is designated. Thus, at step  
19 S23 the cryptography must be performed by the DSA.  
20 Similarly, the conversion of the document to be signed  
21 into summary text must be performed according to the  
22 transformation type (line numbers 9 to 19), and the  
23 calculation of the digest value (line numbers 20 and 21)  
24 must be performed by SHA1. Since the signature template  
25 is canonicalized, it is written using the unicode (UTF-8).  
26 The user terminal 4 transmits the thus obtained signature  
27 value to the agent system 3, and in accordance with the  
28 received signature value the agent system 3 generates a  
29 signed document (step S16). Fig. 7 is a list showing an

1 example signed document. The same information as the  
2 information (<SignedInfo>) entered in the signature  
3 template is written in the signed document, so that it  
4 matches the signature template.

5 "http://www.myagent.com/myorder/2000/0321.xml"

6 (the same value as is added to the signature template) is  
7 added to the target URI, and the digest value (line number  
8 19) and the signature value (line 24) received from the  
9 user terminal 4 are also added. Finally, the public key  
10 information (line numbers 26 to 44) for the signatory is  
11 added to obtain a signed document. The agent system 3  
12 transmits the signed document to the signature demandant  
13 system 2, and the signature demandant system 2 confirms  
14 the contents of the received signed document (step 17).  
15 The signature demandant decrypts the signature value (line  
16 number 24) using the public key information (line numbers  
17 26 to 44) for the signed document. Further, at this time  
18 the signature demandant can employ the signed information  
19 (line numbers 3 to 22) to generate the summary text of a  
20 document and the digest value of the summary text, so that  
21 the hash value before cryptography can be obtained. When  
22 the decrypted hash value and the calculated hash value  
23 match, the legality of the signature can be authenticated.

24 According to the signature method and signature system,  
25 the XML digital signature (XMLDSIG) can be performed using  
26 an information terminal, such as a portable terminal,  
27 having limited calculation resources and a small display

1 screen. According to the system and the method of this  
2 embodiment, since a private key is stored in a portable  
3 information terminal, the terminal can serve as one type  
4 of security token, and the security for the private key  
5 can be improved. Further, since a signatory can confirm  
6 the contents of the summary text on a reliable display  
7 screen, the reliability of the transaction can be  
8 improved.

9 Since the signatory provides a signature only for the  
10 summary text, he or she is responsible only for the signed  
11 summary text. In other words, regardless of what data is  
12 included in the XML document, the responsibility of the  
13 signatory is limited to only the range represented by the  
14 signed summary text. As for the responsibilities of the  
15 agent, the guarantee service can be provided at various  
16 levels depending of the policies of the agent.

17 For example, in some embodiments there is a "non-guarantee  
18 policy". According to this policy, the agent is not  
19 responsible at all for contents other than the data  
20 included with the signature.

21 In addition, in some embodiments there is a  
22 "post-alternation prevention policy". According to this  
23 policy, contents other than those included with the  
24 signature are prevented from being altered later by a  
25 malicious third party. The agent signs the XML document  
26 and stores it, or may request that this operation be  
27 performed by an external authentication service. In some

1   embodiments there is also a "pre-session recording  
2   policy". According to this policy, the agent guarantees  
3   that a series of sessions will be arranged for obtaining  
4   the signature. To do this, a series of interactions for  
5   selecting various options and designating conditions  
6   before the purchase must be performed through the agent.  
7   The agent signs the target document and stores it, while  
8   recording each of these pre-sessions. Even if a malicious  
9   user does attempt to interfere with the transaction,  
10   evidence as to what information was transmitted to the  
11   user terminal is maintained, so that the electronic  
12   commerce site is afforded some guarantee as to contents  
13   other than the signed portion. Meanwhile, since the user  
14   can also be guaranteed that he or she will have any  
15   questions clarified, the user can profess ignorance of  
16   anything that he or she does not recognize.

17   Furthermore, in some embodiments there is a "target  
18   document contents check policy". According to this  
19   policy, the agent employs the profile of the user to  
20   determine whether contents other than the signed portion  
21   includes articles disadvantageous to the user. The  
22   contents of the checking are based on a contract that the  
23   user and the agent execute in advance. If the user is  
24   unsure about the honesty of the agent, the user, uncertain  
25   for a dishonest agent, after the fact, can determine  
26   whether any illegal checks were made by using the post  
27   alteration prevention policy and the external  
28   authentication service.

29   Moreover, since these policies are employed together, the

1 agent can provide a flexible service. The present  
2 invention has been explained by referring to the  
3 embodiment. However, the invention is not limited to the  
4 embodiment, and can be variously modified without  
5 departing from the scope of the invention. In this  
6 embodiment, the private key and the signature template are  
7 stored in the user terminal 4. However, the private key  
8 and the signature template may be recorded on a detachable  
9 storage medium, such as a smart card, and may be read by  
10 loading the storage medium into the terminal 4. Further,  
11 a signature calculation program may also be recorded on  
12 the detachable storage medium, and the above signature  
13 process may be performed by loading this recording medium  
14 into the terminal 4.

15 The typical effects obtained by the invention are as  
16 follows. The XML digital signature can be performed by  
17 using an information processing terminal, such as a  
18 portable terminal, having limited calculation resources.  
19 Further, a more secure, safer digital signature method and  
20 system, or a terminal for digital signature, can be  
21 provided.

22 The present invention can be realized in hardware, software,  
23 or a combination of hardware and software. A visualization  
24 tool according to the present invention can be realized in a  
25 centralized fashion in one computer system, or in a  
26 distributed fashion where different elements are spread  
27 across several interconnected computer systems. Any kind of  
28 computer system - or other apparatus adapted for carrying

1 out the methods and/or functions described herein - is  
2 suitable. A typical combination of hardware and software  
3 could be a general purpose computer system with a computer  
4 program that, when being loaded and executed, controls the  
5 computer system such that it carries out the methods  
6 described herein. The present invention can also be  
7 embedded in a computer program product, which comprises all  
8 the features enabling the implementation of the methods  
9 described herein, and which - when loaded in a computer  
10 system - is able to carry out these methods.

11 Computer program means or computer program in the present  
12 context include any expression, in any language, code or  
13 notation, of a set of instructions intended to cause a  
14 system having an information processing capability to  
15 perform a particular function either directly or after  
16 either or both of the following conversion to another  
17 language, code or notation, and/or reproduction in a  
18 different material form.

19 Thus the invention includes an article of manufacture  
20 comprising a computer usable medium having computer  
21 readable program code means embodied therein for causing a  
22 function described above. The computer readable program  
23 code means in the article of manufacture comprising  
24 computer readable program code means for causing a  
25 computer to effect the steps of a method of this  
26 invention. Similarly, the present invention may be  
27 implemented as a computer program product comprising a  
28 computer usable medium having computer readable program

1 code means embodied therein for causing a a function  
2 described above. The computer readable program code means  
3 in the computer program product comprising computer  
4 readable program code means for causing a computer to  
5 effect one or more functions of this invention.  
6 Furthermore, the present invention may be implemented as a  
7 program storage device readable by machine, tangibly  
8 embodying a program of instructions executable by the  
9 machine to perform method steps for causing one or more  
10 functions of this invention.

11 It is noted that the foregoing has outlined some of the  
12 more pertinent objects and embodiments of the present  
13 invention. This invention may be used for many  
14 applications. Thus, although the description is made for  
15 particular arrangements and methods, the intent and  
16 concept of the invention is suitable and applicable to  
17 other arrangements and applications. It will be clear to  
18 those skilled in the art that modifications to the  
19 disclosed embodiments can be effected without departing  
20 from the spirit and scope of the invention. The described  
21 embodiments ought to be construed to be merely illustrative  
22 of some of the more prominent features and applications of  
23 the invention. Other beneficial results can be realized by  
24 applying the disclosed invention in a different manner or  
25 modifying the invention in ways known to those familiar with  
26 the art.